EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Leo Lenna on 8/6/2007.

The application has been amended as follows:

Claim 1. A method of analyzing and decrypting a malicious encryption script, comprising the steps of:

classifying a malicious script encryption method into a case where a decryption function exists in malicious scripts and is an independent function that is not dependent on ~~the~~ external codes ~~such as run time library~~, a case where a decryption function exists and is a dependent function that is dependent on external codes, and a case where a decryption function does not exist;

if the decryption function exists in malicious scripts and is the independent function that is not dependent on the external codes, extracting a call expression and a

function definition for the independent function, executing or emulating the extracted call expression and function definition for the independent function, and obtaining a decrypted script by putting a result value based on the execution or emulation into an original script at which an original call expression is located;

wherein ~~if the~~ dependency of the decryption function on the external codes is established by determining ~~determined based on whether there exists the dependency of~~ that all codes within the decryption function are dependant on ~~the~~ external codes, that ~~whether~~ actual parameters for decryption function call in all program are constants, and that ~~whether~~ only functions with no side effects in the decryption function are called; and

wherein no ~~if there exists the~~ dependency of all codes within the decryption function on ~~the~~ external codes is established by determining whether all codes within function F_i satisfies the following formula:

$$V_i \cap E_i = \Phi$$

where V_i is a set of global variables defined as used in function F_{i5} and is obtained according to the following formula:

$V_i = A_i - D_i$, and

E_i is a set of variables defined or used in an external region of function F_i and is obtained according to the following formula:

$$E_i = U^{V}_{j}$$

$I \neq j$, $0 \leq j \leq n$

where n is the number of functions defined in the script,

F_1 is an i-th defined function in the script ($1 \leq i \leq n$),

A_1 is a set of all variables defined or used in function F_1 ($1 \leq i \leq n$),

D_1 is a set of all variables declared as Dim in function F_1 ($1 \leq i \leq n$), and

V_0 is a set of variables defined or used in a global region which does not belong to any function.

Please add claim 4 as follows.

Claim 4. The method according to Claim 1 wherein the external codes are run time library.

The examiner's statement of reasons for allowance may be found in the office action mailed 2/27/2007.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ANDREW L. NALVEN whose telephone number is (571)272-3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571 272 3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Andrew L Nalven/
Examiner, Art Unit 2134

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2134
03/05/08